Journal of Signal Processing Systems (2021) 93:323–332
https://doi.org/10.1007/s11265-020-01529-y

Towards Secure and Efficient Scientific Research Project Management Using Consortium Blockchain

Qingfeng Meng[1,2] · **Rungeng Sun**[3]

Received: 15 January 2020 / Revised: 16 February 2020 / Accepted: 3 March 2020 / Published online: 7 April 2020

Abstract
With the development of the knowledge economy, science and technology play an increasingly crucial role in social development. Investment from the government and the enterprise in scientific research has increased significantly, and the number of scientific research projects has also shown an obvious upward trend. Due to the lack of a standardized and unified scientific research project management program, many projects are overdue or even failed, and project fund management is confused. Besides, output results are limited and the actual conversion rate is low. In this paper, we propose a scientific research project management system based on consortium blockchain. Firstly, the process of scientific research project management is standardized. According to this specification, we then design a scientific research project management system in line with consortium blockchain, the smart contract, and the IPFS system. By using these technologies, we have coped with two major problems in traditional scientific project management: breach of contract and confidentiality. The simulation results show that compared with the conventional scientific research project management, the scheme proposed in this paper can significantly enhance the efficiency and the success rate of the project, and reduce the time and manpower consumed in the process of project implementation.

Keywords Research project management · Blockchain · Smart contracts · Consortium blockchain

1 Introduction

Because of socio-economic development and national policy support, the number of scientific research projects in universities, research institutes, and enterprises has gradually increased in recent years. Moreover, the fields involving scientific research projects have become wider and wider, and the funds for scientific research are also increasing, which leads to the higher cost of human communication and supervision in the process of project management. At present, the concept of scientific research project management is relatively backward, lacking a scientific and standardized scientific research project management system. Besides, the informationization level of scientific research management is not high. The following problems are easy to appear: overdue or even failed termination of scientific research projects, illegal use of funds for scientific research projects, leakage of scientific research projects, and low conversion rate of scientific research projects. Therefore, it is of great importance to establish a complete, scientific, standardized, and confidential scientific research project management system.

In terms of an efficient scientific research project management system, the following characteristics are essential: Firstly, it should be normative, dividing the project management into processes, and carrying out research in strict accordance with the process, so as to prevent the occurrence of delayed or even failed scientific research projects. Secondly, a complete quantitative system is in need to quantify the indicators and expected accomplishment goals of scientific research projects. Hence, it can more scientifically explain whether the project meets the expectations in the stage inspection and final result acceptance. It is noteworthy that confidentiality is also very significant. In line with the Regulations on the

✉ Qingfeng Meng
mengqf@nsfc.gov.cn

Rungeng Sun
sunrungeng@outlook.com

[1] Tarim University, Xinjiang, China

[2] National Natural Science Foundation of China, Beijing, China

[3] The School of Computer Science, Beijing Institute of Technology, Beijing, China

Management of Secret Scientific Research Projects of the State Secret Administration, project units must have sound confidentiality systems and organizations to prevent the leakage of scientific research projects and other phenomena.

Currently, the mainstream project management methods include Project Management Body of Knowledge (PMBOK) issued by the Project Management Institute, Project IN Controlled Environment (PRINCE2) of the British Department of Commerce (OGC) [19], and World Wide Project Management Methodology (WW- PMM) [16]. These approaches attempt to standardize the activities of project teams to make prediction, management, and tracking easier.

This paper proposes a scientific research project management system on the basis of consortium blockchain, aiming at standardizing the management of scientific research projects and reducing a range of problems in the scientific research project management. In this system, a scheme to quantify the indicators of scientific research projects is put forward, which can more easily and intuitively view the progress of the project. Combining the traits of consortium blockchain and the smart contract, we believe the system can save the manpower and time cost concerning traditional scientific research project management to the greatest extent. Meanwhile, we use the InterPlanetary File System (IPFS) to manage the files generated in the scientific research project, so as to cut down expenses and ensure the data security.

The primary contributions of this paper are as follows:

1. In combination with the existing project management process system, a scheme to quantify the indicators in scientific research projects is proposed, and algorithms that can approximate the project completion coefficient are given.
2. We design a scientific research project management system in line with consortium blockchain and the IPFS system, which uses the smart contract to regulate the scientific research project management process and employs the IPFS system to solve the problems of data storage and privacy protection in scientific research project management.
3. After making an experiment to test the time consumption of the system, we get the results that the time consumption is only related to the times of requests instead of the file size.

The rest of the paper is organized as follows. We mainly introduce the related research work at home and abroad at this stage in Section 2. In Section 3, we introduce the relevant background knowledge, incorporating scientific research project management, blockchain, the smart contract, and IPFS. Besides, we define the problem; introduce the system model and design objectives in Section 4. Section 5 is the detailed introduction of the research project management system in accordance with consortium blockchain. In Section 6, we use simulation experiments to verify the performance of our system. Finally, we conclude our paper in Section 7.

2 Related Work

At present, there are two widely known project management research systems in the world: the International Project Management Association (IPMA) and the American Project Management Institute (PMI) [8, 27, 35, 36]. In 1996, the PMI released the Project Management Body of Knowledge (PMBOK), which has been updated to the sixth edition in 2017. Furthermore, China's Chinese-Project Management Body of Knowledge (C-PMBOK) has been updated to the second edition, with the content having been expanded and enhanced.

Based on a review and analysis of existing project management literature and other successful disciplines, Frederik Ahlemann et al. have developed a framework to provide guidance for theory-based prescriptive project management, which may help set up viable prescriptive research designs as well [1].

Farzana Asad Mir et al. examined the relationship between project management performance and project success using the experience of project management professionals in UAE project organizations. Research shows that project management performance has a certain relationship with the success of the project, and the organization can improve the success rate of the project by paying more attention to this relationship [21].

Besides, blockchain shines in many application fields with its unique features, such as untamable, anonymous, decentralized, and trustless. Many domestic and foreign blockchain-based applications cover the financial industry, security issues, the Internet of things (IoT), energy, and many other fields [10, 13, 25, 28, 32].

In Massachusetts Institute of Technology, students can use the blockchain technology to manage their own academic record, and they simply need to download an APP called Blockcerts Wallet. In this APP, students can not only view the graduation card but also see credits, professional certificates, and transcripts. This APP is derived from the MIT media lab before publishing a blockchain number of academic certificate blockcerts open standards [12, 17], which have four components of the issuer, the certificate, the verifier, and the wallet.

Al-bassam, Mustafa designed a system called SCPKI based on blockchain to replace the traditional Public Key Infrastructure (PKI) system [20]. Because of its transparent and decentralized design, the system can easily verify

whether certificates are pirated by using smart contracts on Ethereum. Thus, this system with decentralized design can effectively prevent the certificate authority from issuing rogue certificates to the target.

Having combined blockchain with privacy protection, Meng Shen et al. applied it to medical data protection, Internet of things, and other fields [9, 14, 18, 29, 30, 34]

3 Background

3.1 Research Project Management

Project management originated from the United States, among which the critical path method (CPM) and Project Evaluation and Review Technique (PERT) are the representative methods. Over time, more and more standardized project management approaches have emerged, such as PMBOK, PRICNCE2, and WWPMM.

3.1.1 PMBOK

Project management is split into five major processes and ten knowledge areas in line with the Project Management Body of Knowledge (PM- BOK) proposed by the American Project Management Institute (PMI). The ten knowledge areas are: project integration management, project scope management, project time management, project cost management, project quality management, project human resources management, project communication management, project risk management, project procurement management, and project stakeholder management.

3.1.2 PRINCE2

PRINCE2 is the abbreviation for Project IN Controlled Environment. Owned by the Office of Government Commerce (OGC), which was introduced in 1996 and is a structured project management process. The major processes are as follows: Directing a Project (DP), Starting Up a Project (SU), Introducing a Project (IP), Controlling a Stage (CS), Managing Product Delivery (MP), Managing a Stage Boundary (SB), and Closing a Project (CP) [15].

Although the terms used are different, PMBOK and PRINCE2 are highly compatible and complementary. Combining these two project management standards can provide a more efficacious method for our project management. We summarize the project management process as: project initiation, the project declaration, project execution, stage control, and project closure. Besides, project time management, project cost management, and project quality management are involved.

3.2 Blockchain and Smart Contract

3.2.1 Blockchain

Blockchain is a globally maintained and shared distributed ledger, or a distributed global database that can merely be added and viewed [6]. Once a transaction is written to the database, it cannot be deleted or modified. Blockchain includes features, such as decentralization, distrust, data sharing, anonymity, and non-interfering.

Blockchain technology originated from Bitcoin. In November 2008, a self-proclaimed "Satoshi Nakamoto" published the article "Bitcoin: a peer-to-peer electronic cash system" [22], in which he explained how to establish a decentralized peer-to-peer transaction system without a system of trust. Since then, blockchain has entered the public's sight. As of July 30, the total market value of Bitcoin has reached $169 billion, accounting for more than 64% of the total market value concerning all digital cryptocurrencies. Although cryptography itself is highly controversial, the underlying blockchain technology is very valuable, thus being widely used in many fields currently [24].

According to the different access mechanisms, the blockchain falls into three categories: Public Blockchain, Consortium Blockchain, and Private Blockchain. In Table 1, we make a detailed comparison of the three kinds of blockchains [32, 33]

From the features of three different blockchains, we can see that the consortium blockchain is very suitable for the activities with two or a limited number of organizations involved in scientific research projects. The access mechanism and decentralization of the consortium blockchain can increase the confidentiality in the process of scientific research projects to a large extent.

3.2.2 Smart Contract

In reality, the concept of the Smart Contract predates blockchain, which was first proposed by computer scientist and cryptographer Nick Szabo in 1994 [5]. It is described as a series of commitments specified digitally, including agreements for the parties to fulfil. It was not until the concept of blockchain was put forward in 2008 that the smart contract became possible to play a role. However, the smart contract was first widely recognized in 2013 with the birth of Ethereum. In the Ethereum white paper, the smart contract is described as "complex applications involving having digital assets being directly controlled by a piece of code implementing administrative rules" [20].

Technically, a smart contract is a computer program that sets out all the procedures before it is released on the

Table 1 Comperison of three types of Blockchain.

Property	Public blockchain	Consortium blockchain	Private blockchain
Participant	All miners	Designated organizations	Individual or inside an organization
Excitation mechanism	Need	Optional	Unneed
Degree of centralization	Decentralized	Multiple center	Centralized
Speed	Slow	Fast	Fast
Usage scenarios	Cryptocurrency	Business cooperation between organizations	Internal management

blockchain and provides users with an interface through which the program is used. Once the program is published on the chain, it cannot be changed. Instead, it will always run automatically, and the corresponding data will be generated.

The smart contract has the following advantages: (1) accurate execution, (2) low risk of human intervention, (3) decentralization, and (4) low operating cost [7, 11, 23, 31]. Owing to the nature of smart contracts, there are a lot of risks: since smart contracts can't be varied once they are released, there will be irreparable losses if they have holes in the design at the beginning. In May 2016, TheDAO, the largest crowdfunding project for Ethereum in history, completed a $150 million crowdfunding project. However, just one month later, it was attacked by hackers and lost $60 million worth of ETH. Thus, we need to take full advantage of the edges concerning smart contracts while avoiding possible risks.

3.3 IPFS

A complete smart contract system like ethereum, which can be perceived as a programmable distributed database, cannot store large amounts of data on ethereum because of its gas-consuming mechanism. IPFS was a peer-to-peer data distribution protocol whose nodes formed a distributed file system [2–4]. IPFS could be regarded as a single BitTorrent swarm, exchanging objects within one Git repository. Besides, it generates a unique hash value for each file, constructing a map of the hash value to the file. When the file is queried, the basis for the query can be the hash value. Furthermore, IPFS has many advantages in convenience, security, and openness. The combination of IPFS and blockchain provides a feasible alternative to decentralized storage of the growing data.

4 Problem Definition

In this paper,we proposed a scientific research project management system based on consortium chain. The system automatically runs on alliance chain with the smart contract, and it uses the IPFS system to save encrypted files. This section defines problems around system models and design goals.

4.1 System Model

This system establishes the corresponding system around the smart contract and the IPFS system running on the consortium blockchain. As shown in Fig. 1, the entities in the system are split into three categories: institutions participating in the project, the IPFS system, and the consortium blockchain platform. These three sorts of entities realize efficient scientific research project management revolving around the platform of consortium blockchain.

4.1.1 Organizations and Institutions Participating in the Project

The project participants mainly cover the government, universities, enterprises, scientific research institutes, and other organizations or institutions. In this system, they join the consortium blockchain as blockchain nodes.

4.1.2 IPFS System

Due to the restriction of the gas mechanism on the smart contract running on the Ethereum alliance chain, it is unable to store a mass of data files, but a large number of files will be generated during the progress of scientific research projects. The use of IPFS can ensure the existence of data files and the strengthening of its confidentiality.

4.1.3 Consortium Blockchain Platform

The consortium blockchain is more in line with the requirements of project participants for privacy protection, project information protection, and efficient operation. Apart from the project's certain initial attributes, some of the project's progress metrics, time nodes, and hash values

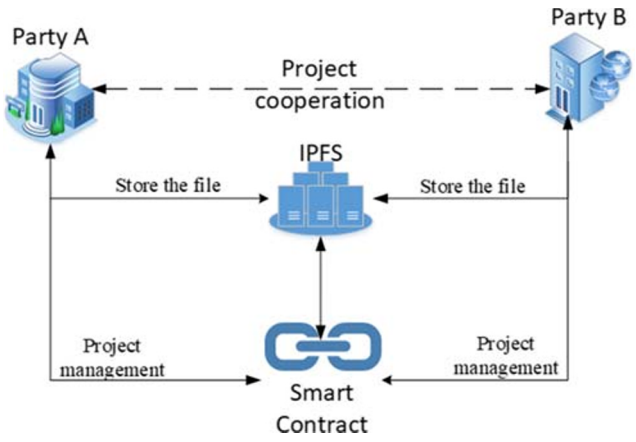

Figure 1 system entity model.

in the IPFS system for files required in the project are also stored on the blockchain.

4.2 Design Goal

Based on consortium blockchain and the IPFS system, this system is a scientific research project management system, with three primary objectives:

1. Security: Because most scientific research projects involve confidential information of countries or enterprises, the security of the management system must be guaranteed.
2. Efficiency: Try to reduce the number of people involved in the management of research projects, and focus on research.
3. Compliance: Prevent project termination or failure due to default of one participant.

In order to achieve the three goals, we chiefly employ the consortium blockchain and IPFS. Once the execution cannot be terminated, all operations in the project will be recorded on the chain block owing to the nature of the smart contract. Moreover, it could not be tampered with and deleted, ensuring the execution of the project and preventing the default of one party. At the same time, the manpower to participate in project management can be lowered. In terms of security issues, the league chain first needs authorization to access the mechanism to a certain degree, so as to protect the safety of the data. For the project file created during the deeper encryption, we combined the IPFS and the asymmetric encryption system to ensure data security and prevent data leakage to the maximum extent.

5 Research Project Management System Based on Consortium Blockchain

5.1 System Overview

The fundamental purpose of this system is to realize the management of the whole process from the project initiation to the end of the project. The realization of this system principally uses the smart contract technology based on the alliance chain and the IPFS system in combination with asymmetric encryption.

The person having access to the system must be an authorized organization or institution, which can join the consortium blockchain as a blockchain node. The grantor can initiate or declare projects initiated by others in the system, and then start scientific research cooperation after establishing a cooperative relationship. In the process of cooperation, all funds transfer, progress inspection tips, and other work will be automatically executed by the smart contract.

5.2 System Module Composition

This system is mainly composed of two functional modules: the data file encryption module and the alliance chain module.

5.2.1 Data File Encryption Module

The file encryption module mostly utilizes the InterPlanetary File System (IPFS) and the asymmetric cryptography. As shown in Fig. 2, when A wants to send the file to B through the blockchain, A first obtains the public key of B, and then use it to encrypt the file. Later, A adds the encrypted file to IPFS using IPFS to acquire the hash value of the file. After the hash value is sent to B through the blockchain, B receives it and obtains the file through IPFS. Then, the hash value will be decrypted with B's own private key to acquire the complete file.

5.2.2 Consortium Blockchain Module

The interaction between project participants is carried out through the alliance chain module. As shown in Fig. 3, the blockchain shared account is made up of blocks linked together in chronological order. Each block contains a number of transactions, in which all the data of the project in a specified format is stored. The format of the stored data is shown in Table 2;

The project data stores all the data of the current project, covering the address of party A and party B, the basic

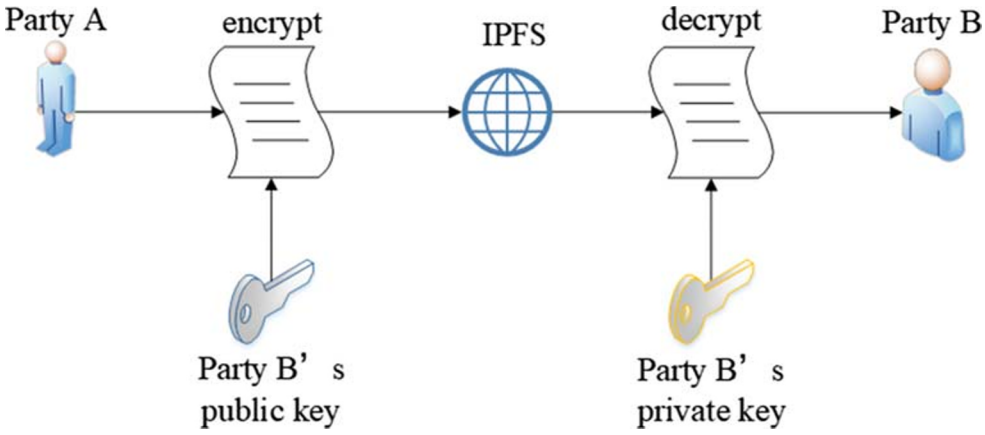

Figure 2 Encrypt module diagram.

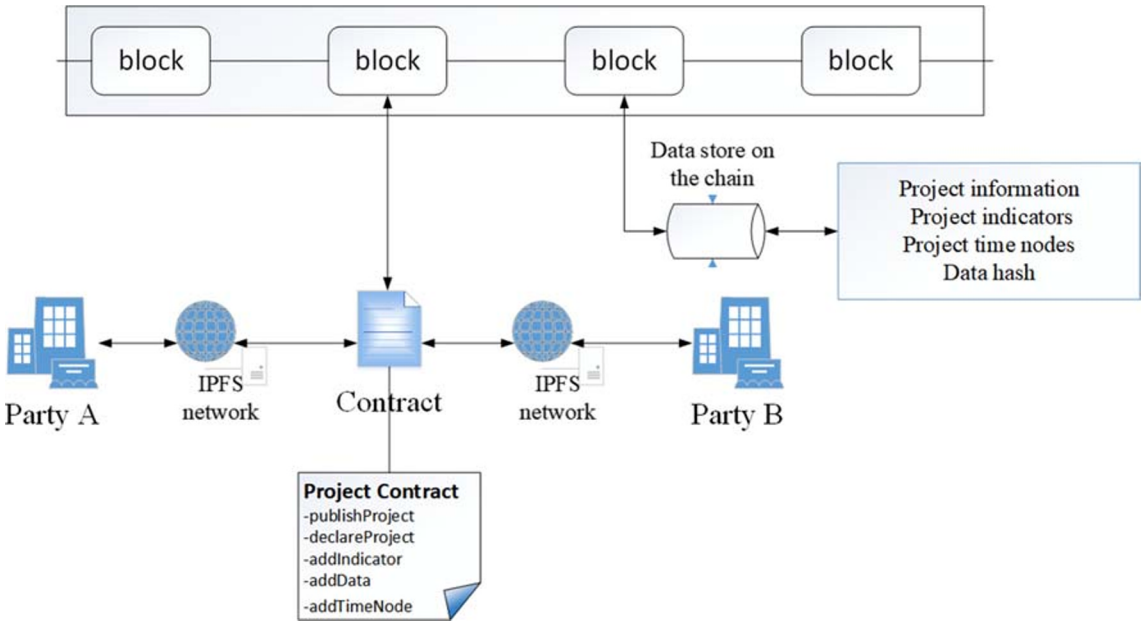

Figure 3 Consortium blockchain module diagram.

Table 2 Data structure of the project on the smart contract.

Property name	Type	Description
Name	string	the project name
partyA	address	the party A's address, party A's balance can be obtained from it
partyB	address	the party B's address, party B's balance can be obtained from it
startTime	uint	start time of the project
endTime	uint	end time of the project
totalFund	uint	total fund of the project
startFund	uint	start fund of the project
timeNodes	TimeNode[]	some time nodes of the project
Indicators	Indicator[]	some progress indicators of the project
Datas	Data[]	the project's datas

information of the project, the time node array of the project, the progress indicator array of the project, and the data files in the project.

- Time Node: contains the name, time, and description of the time node
- Progress Indicator: contains the name, value, type, and description
- Data:contains the name, the source, the public key, hash value, and description

The consortium blockchain model is responsible for the system operation and the data interaction between project participants. Smart contracts will be automatically executed after they are deployed on the blockchain. Notably, the contracts cannot be varied any more, which can effectively prevent the default of project participants.

5.3 System Workflow

The sequence diagram of system workflow is shown in Fig. 4:

Algorithm 1 initializeProject.

Input: startTime, endTime, totalFund, startFund, TimeNodes[], Indicators[]
Output: Transfer project information to the chain

```
project.startTime ← startTime;
project.endTime ← endTime;
project.totalFund ← totalFund;
project.startFund ← startFund;
project.partyA.balance ← project.partyA.balance − project.totalFund
project.balance ← project.totalFund
for i = 0 to m do
    project.timeNodes.push(TimeNodes[i]);
end for
for i = 0 to n do
    project.indicators.push(Indicators[i]);
end for
```

1. Before the project is launched, Party A shall directly upload the project invitation letter and its public key on the IPFS system to the alliance chain for all authorized organizations to check.
2. When C organization or institution intends to cooperate with party A, it will upload the completed project declaration or other materials to the IPFS system using party A's public key encryption. After obtaining the hash value of data, it then writes the hash value and the address of C organization or institution on the consortium blockchain together with the blockchain and sends it to party A.
3. When party A receives the hash of the encrypted file like the project declaration, it first obtains the encrypted project declaration and other materials through the IPFS system. Then, party A uses its private key for decryption and get the real document. According to the project declaration, audit declaration will be discussed. If party A agrees to cooperate with C tissue for the scientific research project, Algorithm 1 is needed to initialize some of the project properties, including: the address of the party A and party B, project start time, the end of the project time, total project funds, startup capital, some sorted time node (used for achievement inspection), and some custom project indicators. Then, party A needs to transfer the total scientific research fund into the contract, encrypt the project contract with party B's public key, upload it to the IPFS system, and pass the hash value to the chain. When party A's initialization is completed, party B will receive the initialization information of the project.
4. When party B agrees that the information of the project is correct, the project will start and the smart contract will automatically transfer the specified start-up fund to party B's address.

Algorithm 2 checkSchedule.

Input: Project, Indicators[]
Output: result

```
i ← 0;
result ← true;
while i ← indicators.length do
    indicator ← indicators[i];
    if indicator.type == 0 then
        if indicator.value > project.indicators[i].value then
            result ← false;
            BREAK;
        end if
    else
        if indicator.value > project.indicators[i].value then
            result ← false;
            BREAK;
        end if
    end if
    i++;
end while
return result, indicators[];
```

5. As the time node is reached, the contract shall send a request to party B. At this time, party B will send the results of the current stage to the blockchain in accordance with the specified index style. This contract

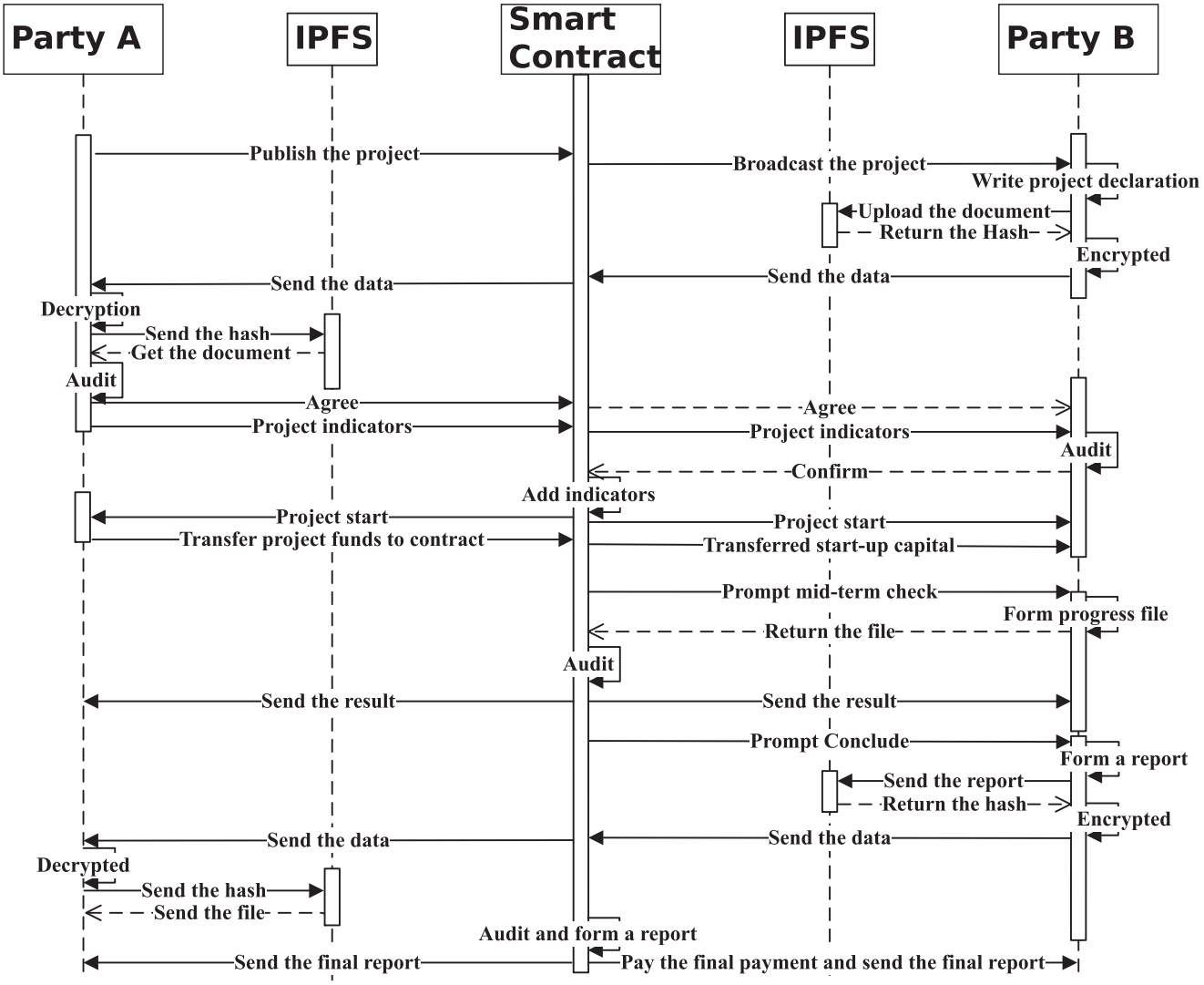

Figure 4 System sequence diagram.

shall calculate the project progress currently completed by party B through algorithm 2, input in algorithm 2 is 'Project' and 'Indicators', where 'Project' refers to the progress of the current Project and 'Indicators' refers to the set Project Indicators. The results will be sent to party A and party B by the contract.

6. When the final conclusion time node is reached, party B shall encrypt the conclusion report and other materials with party A's public key and upload them to the IPFS system. The obtained hash value together with party B's current progress should be sent to the chain. After the completion situation of party B is calculated in the contract, the completion result and the hash value of the encrypted material shall be sent to party A together. If the expected situation is not met, party A may adjust the deadline to wait for party B's completion based on the actual situation, or declare that the project is a failure. If so, the remaining funds will be transferred back to party A's address. If party B achieves the expected goal, party A shall confirm the completion of the project.
7. When project-related data and logs are sent to party A and party B by the smart contract, the project is over.

6 Performance Evaluation

The combination of consortium blockchain, IPFS, and asymmetric encryption fully guarantees the security of the system. Writing smart contracts in the solemotion language enables the management of the whole process from project declaration to the project conclusion. As the smart contract is deployed to the Ethereum alliance chain platform, each

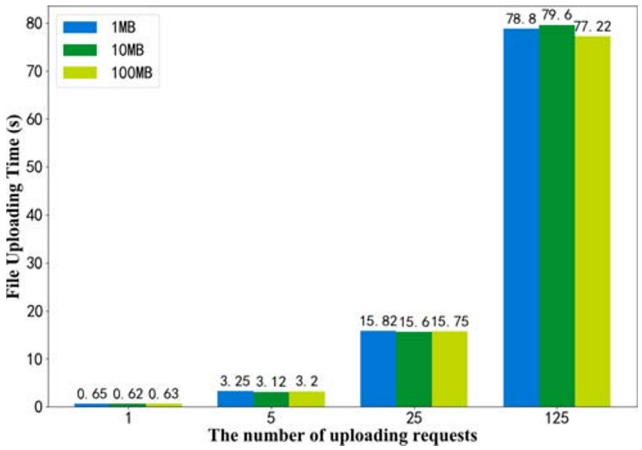

Figure 5 Response time diagram.

organization or institution corresponds to one alliance chain node, which can invoke the smart contract through the console.

We used a PC to simulate an organization participating in the project, and tested its response time to the system request. The request times were 1, 5, 25, and 125 times, respectively. Besides, the size of file data involved in each request was 1 MB, 10 MB, and 100 MB, respectively. A PC representing a project participant is configured as: Intel(R) Core(TM) i5-8300h CPU @2.30ghz 2.30ghz, 8GB RAM and 64-bit window OS.

In our experiment, we focus on evaluating the file uploading time, as it is a crucial performance indicator of the project management systems. The file uploading time with different uploading requests as well as file sizes is exhibited in Fig. 5. We can see that even a 100MB file can be uploaded in around 0.6s, which meets the needs of practical applications. We also observe that the file uploading time is almost irrelevant to file size. This is because the hash value returned by IPFS network is not large. The main factor that affects the uploading time is the number of uploading requests, i.e., the file uploading time is proportional to the number of files. For instance, the uploading time of 1, 5, 25, 125 requests for a 10MB file are 0.62s, 3.12s, 15.63s, and 79.6s, respectively.

Compared with the traditional method of transferring documents manually in scientific research project management, this system saves manpower, material resources and time greatly on the premise of ensuring its security.

7 Conclusion

The purpose of this paper is to implement an efficient scientific research project management system. By using the data of tamper-resistant consortium blockchain with automatic smart contract execution and default, as well as the characteristics of distributed global file database IPFS, the system implements a feasible scientific research project management system. Through the simulation test, the system can standardize scientific research project management flow, effectively reduce the time of the scientific research project management and human capital, strengthen its privacy, and improve the success rate of the scientific research project.

In future work, we plan to enhance our system and conduct more detailed experiments to verify the safety and security of our system [26, 37].

References

1. Ahlemann, F., Arbi, F.E., Kaiser, M.G., Heck, A. (2013). A process framework for theoretically grounded prescriptive research in the project management field. *International Journal of Project Management*, *31*(1), 43–56. https://doi.org/10.1016/j.ijproman.2012.03.008. The International Network for Business and Management Journals (INBAM) 2012.
2. Ali, M.S., Dolui, K., Antonelli, F. (2017). Iot data privacy via blockchains and ipfs. In *Proceedings of the seventh international conference on the internet of things* (p. 14): ACM.
3. Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. arXiv:1407.3561.
4. Brito, I.P., Tropaldi, L., Carbonari, C.A., Velini, E.D. (2018). Hormetic effects of glyphosate on plants. *Pest Management Science*, *74*(5), 1064–1070.
5. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, *4*, 2292–2303.
6. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., et al. (2016). Blockchain technology: beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.
7. Dai, P., Mahi, N., Earls, J., Norta, A. (2017). Smart-contract value-transfer protocols on a distributed mobile application platform. https://qtum.org/uploads/files/cf6d69348ca50dd985b60425ccf282f3.pdf p. 10.
8. Eberle, A., Meyer, H., Rosen, D. (2011). A comparison of pmi and ipma approaches. Analysis to support the project management standard and certification system selection.
9. Gao, F., Zhu, L., Shen, M., Sharif, K., Wan, Z., Ren, K. (2018). A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. *IEEE Network*, *32*(6), 184–192.
10. Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*, *2*(1), 24.
11. Hahn, A., Singh, R., Liu, C.C., Chen, S. (2017). Smart contract-based campus demonstration of decentralized transactive energy auctions. In *2017 IEEE Power & energy society innovative smart grid technologies conference (ISGT)* (pp. 1–5): IEEE.
12. Hope, J. (2018). Issue secure digital credentials using technology behind bitcoin. *The Successful Registrar*, *17*(11), 1–4.
13. Hukkinen, T., Mattila, J., Ilomäki, J., Seppälä, T., et al. (2017). A blockchain application in energy. *ETLA Reports*, 71.
14. Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., Yu, N. (2019). Healthchain: a blockchain-based privacy preserving scheme for large-scale health data. *IEEE Internet of Things Journal*, *6*(5), 8770–8781.
15. Jamali, G., & Oveisi, M. (2016). A study on project management based on pmbok and prince2. *Modern Applied Science*, *10*(6), 142–146.

16. Jessup, C.B., Moore, S.C., Palozzi, G., Stefanski, P.A., Trisko, S.D., Wilkie, L.E. (2010). Method, system and program product for assessing a product development project employing a computer-implemented evaluation tool. US Patent 7,680,682.
17. Jirgensons, M., & Kapenieks, J. (2018). Blockchain and the future of digital learning credential assessment and management. *Journal of Teacher Education for Sustainability*, *20*(1), 145–156.
18. Shen, M., Ma, B., Zhu, L., Mijumbi, R., Du, X., Hu, J. (2017). Cloud-based approximate constrained shortest distance queries over encrypted graphs with privacy protection. *IEEE Transactions on Information Forensics and Security*, *13*(4), 940–953.
19. Matos, S., & Lopes, E. (2013). Prince2 or pmbok–a question of choice. *Procedia Technology*, *9*, 787–794.
20. McCorry, P., Shahandashti, S.F., Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy. In *International conference on financial cryptography and data security* (pp. 357–375): Springer.
21. Mir, F.A., & Pinnington, A.H. (2014). Exploring the value of project management: linking project management performance and project success. *International Journal of Project Management*, *32*(2), 202–217.
22. Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. http://www.bitcoin.org/bitcoin.pdf. (cited on pp. 15 and 87) (2017).
23. Savelyev, A. (2017). Contract law 2.0:'smart'contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*(2), 116–134.
24. Shen, M., Deng, Y., Zhu, L., Du, X., Guizani, N. (2019). Privacy-preserving image retrieval for medical iot systems: a blockchain-based approach. *IEEE Network*, *33*(5), 27–33.
25. Shen, M., Tang, X., Zhu, L., Du, X., Guizani, M. (2019). Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities. *IEEE Internet of Things Journal*.
26. Shen, M., Zhang, J., Zhu, L., Xu, K., Tang, X., Liu, H. (2019). Security svm training over vertically-partitioned datasets using consortium blockchain for vehicular social networks. *IEEE Transactions on Vehicular Technology*, 1–10.
27. Toljaga-Nikolić, D., Obradović, V., Mihić, M. (2011). Certification of project managers based on ipma and pmi models through conforming to iso 17024: 2003 1. *Management* (1820-0222) (59).
28. Turk, Ž., & Klinc, R. (2017). Potentials of blockchain technology for construction management. *Procedia Engineering*, *196*, 638–645.
29. Guan, Z., Zhang, Y., Zhu, L., Wu, L., Yu, S. (2019). Effect: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid. *Science China Information Sciences*, *62*(3), 32103.
30. Guan, Z., Liu, X., Wu, L., Wu, J., Xu, R., Zhang, J., Li, Y. (2020). Cross-lingual multi-keyword rank search with semantic extension over encrypted data. *Information Sciences*, *514*, 523–540.
31. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., Wan, J. (2018). Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal*, *6*(2), 1594–1605.
32. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2017). An overview of blockchain technology: architecture, consensus, and future trends. In *2017 IEEE International congress on big data (BigData congress)* (pp. 557–564): IEEE.
33. Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, *14*(4), 352–375.
34. Zhu, L., Tang, X., Shen, M., Du, X., Guizani, M. (2018). Privacy-preserving ddos attack detection using cross-domain traffic in software defined networks. *IEEE Journal on Selected Areas in Communications*, *36*(3), 628–643.
35. Qiu, M., Sha, E.H.-M., Liu, M., Lin, M., Hua, S., Yang, L.T. (2008). Energy minimization with loop fusion and multi-functional-unit scheduling for multidimensional dsp. *Journal of Parallel and Distributed Computing*, *68*(4), 443–455.
36. Li, J., Ming, Z., Qiu, M., Quan, G., Qin, X., Chen, T. (2011). Resource allocation robustness in multi-core embedded systems with inaccurate information. *Journal of Systems Architecture*, *57*(9), 840–849.
37. Shao, Z., Xue, C., Zhuge, Q., Qiu, M., Xiao, B., Sha, E.H.-M. (2006). Security protection and checking for embedded system integration against buffer overflow attacks via hardware/software. *IEEE Transactions on Computers*, *55*(4), 443–453.